doi:10.3788/gzxb20124111.1365

一种保持非负整数值的图像加密算法

吕善翔[1],王兆山[1],盛堰[2],冯久超[1]
(1 华南理工大学 电子与信息学院,广州 510641)
(2 广州海洋地质调查局,广州 510760)

摘 要:提出了一种能够使双随机相位图像加密方法的密文图像保持为非负整数值的变换——重构变换.重构变换包括预处理和频谱搬移两个过程,其主要特点为,在图像进行频域变换之前,通过叠加的方式将整数图像压缩成一半大小的复数图像,从而能缩小后续运算的计算空间;基于重构变换的双随机相位图像加密方法可以实现联合图像压缩和加密的效果.与基于混沌系统的数字图像加密方法相比,本文方法的密文图像具有更低的信息熵.实验结果表明,该方法具有较强的安全性,解密图像基本无失真,并且密文图像对加性噪音攻击具有一定的鲁棒性.

关键词:光学图像;数字图像;复数;非负整数
中图分类号:TN957.52 **文献标识码**:A **文章编号**:1004-4213(2012)11-1365-7

0 引言

近年来,互联网技术飞速发展,在网络上传送音频、视频和图像等多媒体信息的需求也日益增多,与此同时,人们对互联网信息传送过程中的安全性和保密性要求也越来越高.加密方法是对信息进行编码和解码的方法,对图像信息的加密方法可以分为三大类:1) 把图像当作普通的二进制文件来进行加密.这种加密方法可以使用包括 DES、AES 等传统的密码学算法来进行[1-3],但这种方法没有考虑到图像信息的特征,加密图像信息的微小失真会导致解密失败;2) 用图像处理技术的加密方法.其中又包括时域加密和频域加密 2 个子类:①时域加密.典型方法是利用混沌系统来对图像进行像素置乱以及灰度置乱[4-6];②频域加密.主要是采用分数阶傅里叶变换(Fractional Fourier Transform, FRFT)来对图像进行加密[7-9],因为 FRFT 的变换阶数可以作为图像加密的密钥,但该方法的加密结果是复数;3) 利用光学信息处理技术进行加密,指的是利用光学加密理论来进行数字图像加密处理.例如利用双随机相位的方法(Double Random Phase Encryption, DRPE)来加密图像[10-14],但该方法的加密结果也为复数,不利于图像的存储及传输,因而该加密方法主要在光学图像加密的计算机仿真时应用.

有不少学者研究如何建立一种实值图像加密方法,从而可以减少加密图像的信息熵.现阶段主要有三种实值加密方法:1)将加密图像的存储空间扩大[15-16],但是需要存储及传输的数据量也对应增大,因此这种方法的效率不高;2)利用希尔伯特变换,将图像压缩成二分之一的频域图像来进行处理[17],最后再把图像还原到实数域;3)基于保持实值的分数阶傅里叶变换[18]来进行图像加密.上述三种方法的加密结果都是在一个很大区间内分布的正数和负数的集合矩阵,不利于保存成数字图像.

本文提出了一种能够使双随机相位图像加密方法的密文图像保持为非负整数值的变换——重构变换.基于重构变换的双随机相位图像加密方法可以实现联合图像压缩和加密的效果.本文首先介绍图像重构变换的实现方法,并对其算法复杂度进行分析.之后,介绍重构变换在双随机相位图像加密方法中的应用,也即是实现了一种基于变换域的数字图像加密方法.最后,对保持非负整数值的双随机相位图像加密方法进行了实验分析,实验结果表明本文加密方法可以减少密文图像的信息熵和数据量并保持密文图像的安全性,且具有较大的密钥空间,密文图像对于高斯噪音干扰和椒盐噪音干扰具有较强的鲁棒性.

1 重构变换

1.1 算法引入

重构变换包括预处理和频谱搬移两个过程.对于一幅具有 256 级灰度的图像,预处理的步骤可以

基金项目:国家自然科学基金(No. 60872123)和国家-广东省自然科学基金联合基金(No. U0835001)资助
第一作者:吕善翔(1988—),男,硕士研究生,主要研究方向为混沌信号处理,数字图像处理. Email:lvshanxiang@126.com
责任作者/导师(通讯作者):冯久超(1964—),男,博导,博士,主要研究方向为非线性电路、混沌信号与信息处理. Email:fengjc@scut.edu.cn
收稿日期:2012-06-17;**修回日期**:2012-09-12

记为以下两步：

Step1：设原图像 $h(x_1,y_1)$ 的大小为 $M\times N$，将 $h(x_1,y_1)$ 按上下对半的方式拆开为

$$h(x_1,y_1)=\begin{cases}h(x_1,y_1)_{\text{up}} & x=1:\dfrac{M}{2},y=1:N\\ h(x_1,y_1)_{\text{down}} & x=\left(\dfrac{M}{2}+1\right):M,y=1:N\end{cases} \tag{1}$$

Step2：将 $h(x_1,y_1)_{\text{up}}$ 当成图像的实部，$h(x_1,y_1)_{\text{down}}$ 当成虚部，构造一幅 $\dfrac{M}{2}\times N$ 的复数图像，从而减少图像的运算空间.

$$H(x_2,y_2)=\frac{1}{k}(h(x_1,y_1)_{\text{up}}+\text{j}h(x_1,y_1)_{\text{down}}) \tag{2}$$

式中 k 称为缩放因子，当 $k\in[3,4]$ 时，解密的图像能够获得较高的恢复质量. 缩放因子的作用是，减少密文图像的值域区间.

在经过预处理之后，复数图像 $H(x_2,y_2)$ 可以进行传统的加密运算. 为了使运算结果转化为 256 级灰度值，在复数域的加密运算之后需要进行频谱搬移，其步骤如下：

Step1：假设经过复数域处理之后的图像是大小为 $\dfrac{M}{2}\times N$ 的 $G(x_2,y_2)$，分别提取其实部和虚部，即

$$\begin{aligned}h_2(x_1,y_1)_{\text{up}}&=\text{real}(G(x_2,y_2))\\ h_2(x_1,y_1)_{\text{down}}&=\text{imag}(G(x_2,y_2))\end{aligned} \tag{3}$$

Step2：将图像拼接成为 $M\times N$ 的 256 级灰度图像 $h_2(x_1,y_1)$.

$$h_2(x_1,y_1)=\left[\begin{pmatrix}h_2(x_1,y_1)_{\text{up}}\\ h_2(x_1,y_1)_{\text{down}}\end{pmatrix}+d\begin{pmatrix}1&\cdots&1\\ \vdots&\ddots&\vdots\\ 1&\cdots&1\end{pmatrix}\right] \tag{4}$$

式中，[] 表示取整，d 称为搬移系数，当缩放因子 k 不同时，它会对应有不同的最优值.

图像重构变换的特点体现在以下几个方面：1）通过叠加的方式将整数图像压缩成一半大小的复数图像，从而能缩小后续运算的计算空间；2）缩放因子 k 的引入，使密文图像的值控制在 [−128 128] 之间，最后通过 d 参量将密文图像值域移到 [0 255]；3）频谱搬移过程中，取整这一步骤会使重建的图像产生微小失真，但这些失真可以减少密文图像所需要保存的数据量，在加密的同时实现了压缩的效果；4）缩放因子和搬移系数对应不同的图像会有不同的联合最优值，在实验分析中我们将对其进行探讨.

1.2 算法复杂度分析

在重构变换中，预处理需要进行 $\dfrac{M}{2}\times N$ 次的加法运算，频谱搬移需要 $(\dfrac{M}{2}\times N+M\times N)$ 次的加法运算，因此重构变换的运算复杂度只有 $O(2M\times N)$. 由上述分析可知本算法的运算复杂度很低.

2 数字图像的双随机相位加密方法

光学信息处理方法能够实现高速的并行处理、抗干扰能力强以及光速运算等优点. 在光学图像加密方法中，双随机相位加密应用最为广泛，然而，该加密方法在数字图像加密中并不可行，因为它复数的加密结果包含了太多冗余信息. 如果给合本文所提出的重构变换，那么光学加密理论中的双随机相位加密方法则能应用于数字图像加密.

光学图像的双随机相位加密过程如图 1 所示.

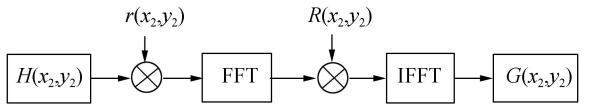


图 1 双随机相位加密流程

Fig. 1 The flowchart of DRPE

设原始图像为 $H(x_2,y_2)$，$r(x_2,y_2)$，$R(x_2,y_2)$ 是随机相位掩膜，$r(x_2,y_2)=\exp(\text{i}2\pi r_0(x_2,y_2))$，$R(x_2,y_2)=\exp(\text{i}2\pi R_0(x_2,y_2))$，$r_0(x_2,y_2)$ 和 $R_0(x_2,y_2)$ 都是取值范围在（0，1）的随机数. $H(x_2,y_2)$ 是加密之后的复数图像.

将重构变换应用到双随机相位加密方案中，则光学加密系统的加密流程如图2所示. 其中加密步

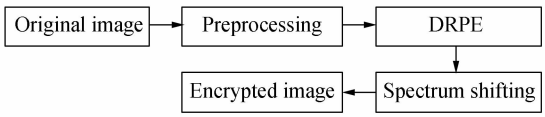


图 2 基于重构变换的双随机相位加密流程

Fig. 2 The flow chart of double random phase encryption based on reconstruction transform

骤为：

Step1：对于一幅 $M\times N$ 灰度图像 $h(x_1,y_1)$，通过图像重构变换中的预处理变换成 $\dfrac{M}{2}\times N$ 的复数图像 $H(x_2,y_2)$.

Step2：用双随机相位方法将 $H(x_2,y_2)$ 加密成 $G(x_2,y_2)$. 双随机相位加密后的图像 $G(x_2,y_2)$ 可以表示为

$$G(x_2,y_2)=\text{IFFT}(\text{FFT}(H(x_2,y_2)\cdot \exp(\text{i}2\pi r_0(x_2,y_2)))\exp(\text{i}2\pi R_0(x_2,y_2))) \tag{5}$$

Step3：将图像 $G(x_2,y_2)$ 通过频谱搬移转换成为 $M\times N$ 的 $h_2(x_1,y_1)$，其中 $h_2(x_1,y_1)$ 是在 0 至 255 之间的非负整数. 因此，$h_2(x_1,y_1)$ 易于保存为数字图像并且在网络上传输非常方便.

解密步骤是加密步骤的逆过程. 因为重构变换只是一些线性变换，所以本文所提出的保持非负整数双随机相位图像加密方案的光学实现在理论上也是可行的.

3　实验结果

为了验证重构变换算法的效率，我们在 MATLAB7.0 环境下使用 Lena 图像及 hill 图像，对基于重构变换的双随机相位图像加密方法进行分析，所使用图像灰度级别为 256，大小是 256×256.

3.1　加密图像的信息熵

为了衡量加密前后图像包含的信息量是否有变化，这里引入信息熵来进行度量. 设图像矩阵的大小为 $M\times N$，矩阵的信息熵可写为

$$H=-\sum_{i=0}^{255}P(i)\log_2 P(i) \tag{6}$$

式中 0 和 255 分别为该灰度图像像素的最大值和最小值，$P(i)$ 是数值为 i 的元素在矩阵中出现的概率. 基于信息熵，传输数据的总比特数可以写为

$$D=M\times N\times H \tag{7}$$

注意到式(7)对灰度图像的信息熵求解是针对整型值来说的，若图像是复数图像或非整型值图像，则需要通过分段统计的办法来计算信息熵.

为了体现本文所提方案的特点，在表 1 中引入了其它典型的加密方案在密文图像的信息熵方面的表现性能，以进行比较. 其中，文献[15]是双随机相位加密图像方法中保持密文实值的代表，文献[19]是利于混沌系统来对图像进行位置乱的加密方法，文献[20]是将图像的置乱和扩散操作联合起来的混沌加密方法.

表 1　本文方法与其它图像加密方法的比较

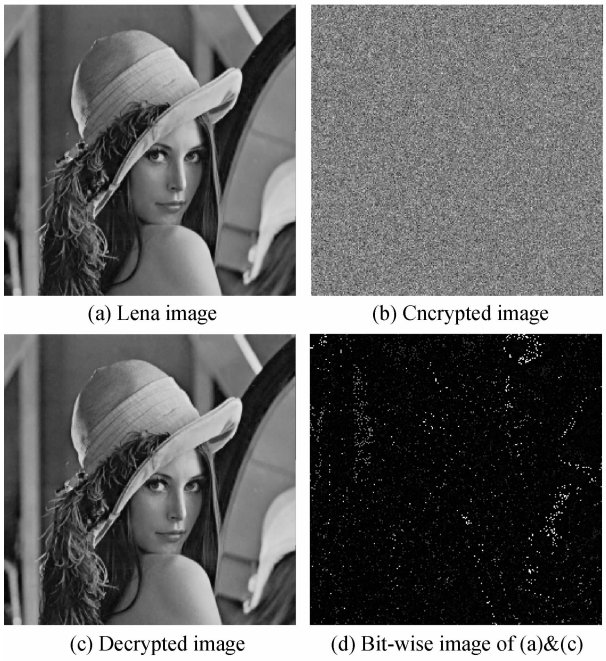
Table 1　Comparison of our scheme and other image encryption schemes

	Information entropy	Data volume
Original Lena	7.57	7.57×256^2
Our scheme	6.85	6.85×256^2
Scheme in [15]	10.25	10.25×512^2
Scheme in [19]	7.99	7.99×256^2
Scheme in [20]	7.99	7.99×256^2

对于一幅具有 256 级灰度的整型值图像来说，其最大信息熵是 $\log_2 2^8=8$. 在表 1 中，文献[15]的方法计算所得信息熵大于 8，是因为其密文图像是非整数图像，信息熵计算采用 2 560 个分段近似计算：统计像素值在每一段的出现频率，再计算其信息熵. 又因其密文图像大小是原文的 4 倍，该方法需要传输的数据量非常大.

在表1中，文献[19]和[20]的方法都是利用混沌系统来加密图像的方法，这类方法能使密文图像具有趋于 8 的信息熵，但其劣势在于不易于图像压缩方法相结合. 因为好的混沌加密方法都会具有较好的雪崩效应(一个原始图像像素位的改变会导致密文图像大部分像素位的改变). 由此，如果再将这些加密方法的密文图像进行有损压缩(比如变换编码，小波编码)，则由压缩之后的图像无法恢复出原始图像.

本文方法的加密图像具有比原始图像更小的信息熵，实现了图像压缩与加密的联合. 本文方法信息熵降低的原因是在进行重构变换的过程中，式(4)的取整运算丢弃了小数部分的信息. 从图 3(c)可以看到，本文方法的解密图像与原文图像的差别是人眼难以区分的. 另外，从图 3(d)可以看出，本文加密方法所减少的信息熵对应着解密图像的小部分轮廓信息丢失.



(a) Lena image　(b) Cncrypted image

(c) Decrypted image　(d) Bit-wise image of (a)&(c)

图 3　解密图像和原始图像的差别

Fig. 3　The difference between the decrypted image and the original image

3.2　缩放因子 k 及搬移系数 d 的最优值

为了评估本方法恢复的图像质量，我们使用峰值信噪比(Peak Signal Noise Ratio，PSNR)，这一参量来进行测量. PSNR 的定义式为

$$\mathrm{PSNR}=10\log_{10}\frac{D'^2MN}{\sum_{m=1}^{M}\sum_{n=1}^{N}(I(m,n)-I'(m,n))^2}\mathrm{d}B \tag{8}$$

其中 $I(m,n)$ 是原始图像的灰度值，$I'(m,n)$ 是恢复图像的灰度值，两幅图像的大小都为 $M\times N$，D' 是图像灰度级别的最大值.

为了测量缩放因子 k 对加密效果的影响，我们先将搬移系数 d 固定为常量，将 k 设置为在[2.5 5.5]内的自变量，对应的 PSNR 值为因变量，加密效果如图 4 所示.

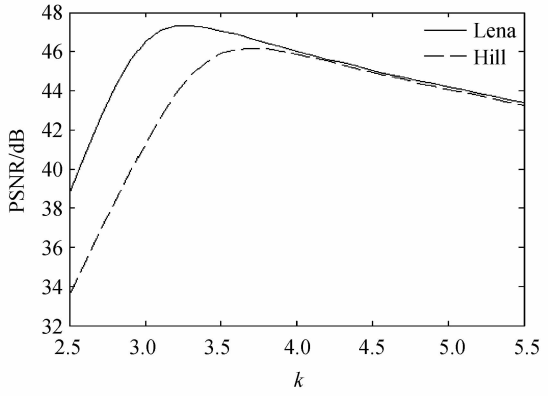


图 4 缩放因子 k 对 PSNR 的影响

Fig. 4 The influence of scaling factor k on PSNR

在图 4 当中，Lena 图像对应的最优 k 值是 3.2，hill 图像对应的最优 k 值是 3.7. 当 k 在[3 4]内取值时，恢复图像与原图像的峰值信噪比都大于 40 dB，这时恢复图像与原图像的差别是人眼难以分别的，因而使用重构变换的方法来改良双随机相位加密具有实用性. 如果将式(4)里面取整这一运算步骤去除，从加密结果就能够无失真地恢复原图，但是加密的非整数图像无法保存成位图文件. 在另一方面，当缩放因子 k 越大，本文方案所加密图像的信息熵越小，其对原始图像的有损压缩率也就越高.

同理，为了测量搬移系数 d 对加密效果的影响，我们可以将 k 固定为最优值区间内的 3.5，然后以 d 在[113 143]区间内作为自变量，观察其加密所对应的 PSNR 值变化，变化效果如图 5 所示.

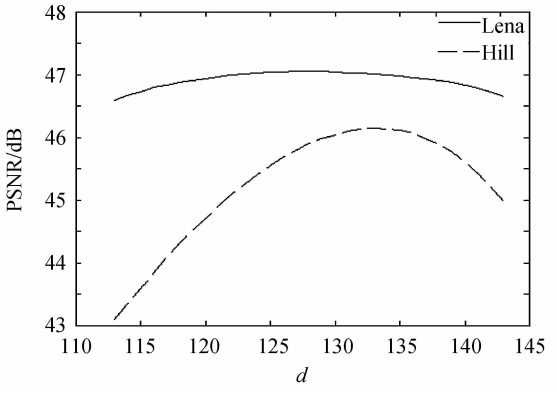


图 5 搬移系数 d 对 PSNR 的影响

Fig. 5 The influence of shifting factor d on PSNR

在图 5 中，当 d 取 128 时，Lena 图像对应有最大的 PSNR 值，当 d 取 134 时，Hill 图像对应有最大的 PSNR 值. 从图 5 可以看出，Hill 图像对搬移系数的变化较Lena图像敏感，原因是，式(4)的取整运算对于信息熵更小的图像影响更大.

对于一幅特定图像来说，如何求解 k 和 d 的联合最优值是一个求解二维多峰函数的全局最优值问题，可以采用群智能优化算法来进行快速求解(比如人工蜂群算法). 然而，如果在加密图像之前都采用优化算法来求出其联合最优值，则不能保证加密方案的实时性. 由于当 k 在[3 4]内取值，d 在[125 135]内取值时，解密图像都能取得 40 dB 以上的峰值信噪比，因此，我们可以确立一个“联合最优区间”的概念，当 k 和 d 在联合最优区间内取值时($k\in[3,4]$，$d\in[125,135]$)，解密图像的微小失真是人眼不可见的. 这种在联合最优区间内取值的方法可以实现对不同图像的快速、高效加密.

3.3 安全性分析

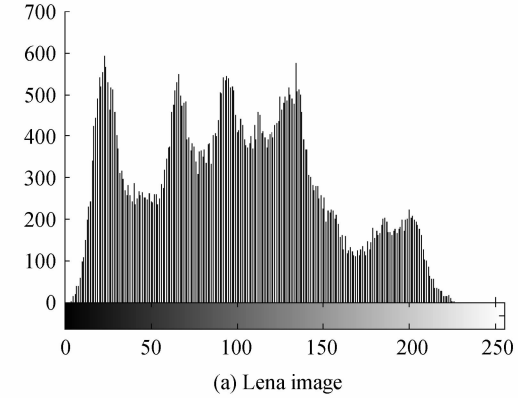
为了对本方法的安全性进行验证，将缩放因子 k 和搬移系数 d 在最优区间内分别取 3.5 和 128，然后考察本文加密方法的密钥空间，以及对其进行统计分析.

3.3.1 密钥空间分析

图像加密算法的密钥空间一般要足够大，从而能够抵抗穷举攻击. 对于本文提出的加密算法，其密钥空间分析如下：随机相位板的每一个密钥位在 MATLAB7.0 上执行时都是双准确度实数，假设输入图像的大小为 $M\times N$，则本文方法对应的密钥空间为 $2\times10^{15\times M\times N}$，假设尝试一次可能解所需的时间是 1 秒，则穷举一幅 256×256 密文图像所需要的时间是：$\frac{2\times10^{15\times256\times256}}{3.15\times10^{7}}\approx0.63\times10^{8\times256\times256}$ 年，该密钥空间是足够大的.

3.3.2 柱状图分析

加密前后的柱状图如图 6 所示. 从上图可以看出，加密之后图像的像素值近似于正态分布. 本方法加密的任何图像都是这种近似正态的分布，因此这种分布的安全性不比均匀分布的安全性低.



(a) Lena image

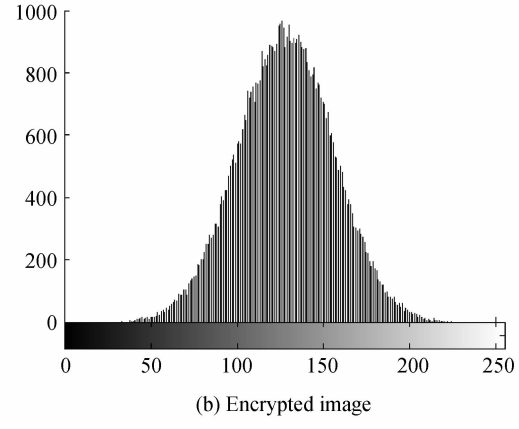


图 6　Lena 图像加密前后的统计直方图

Fig. 6　The statistic histogram of Lena image and the encrypted image

3.3.3　邻域像素相关性分析

分别从水平、垂直、对角三个方向来分析加密之后图像的相关性. 为了提高计算效率，我们随机选取 4000 对像素点进行分析，其中计算像素相关性的公式为

$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i, E(y)=\frac{1}{N}\sum_{i=1}^{N}y_i \tag{9}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2, D(y)=\frac{1}{N}\sum_{i=1}^{N}(y_i-E(y))^2 \tag{10}$$

$$\mathrm{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{11}$$

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{12}$$

式中 x 和 y 分别表示图像中随机选出的像素对的两个灰度值，r_{xy} 为图像的像素相关性. 从表 2 可以看到，原始 Lena 图像在 3 个方向的像素相关性都非常高，而加密之后的像素相关性都是负数，从而表明改进的双随机相位图像加密方案安全性高. 图 7 为图像垂直方向的像素相关性.

表 2　原文和密文的邻域像素相关性

Table 2　Adjacent pixel correlations of plaintext and ciphertext

Directions	Original image	Cipher-text image
Horizontal	0.938 5	−0.024 5
Vertical	0.969 3	−0.011 0
Diagonal	0.916 4	−0.017 3

3.4　抗干扰性能

用图像处理的办法来加密图像的一个显著优点就是这种方法能抵抗一定的加性噪音干扰. 对 Lena 图像应用本文方法进行加密，再对密文图像分别加上 0.001 dB 的高斯噪音和 0.001 dB 的椒盐噪音，如图 8(a)，(c)所示. 对于被噪音污染之后的图像，

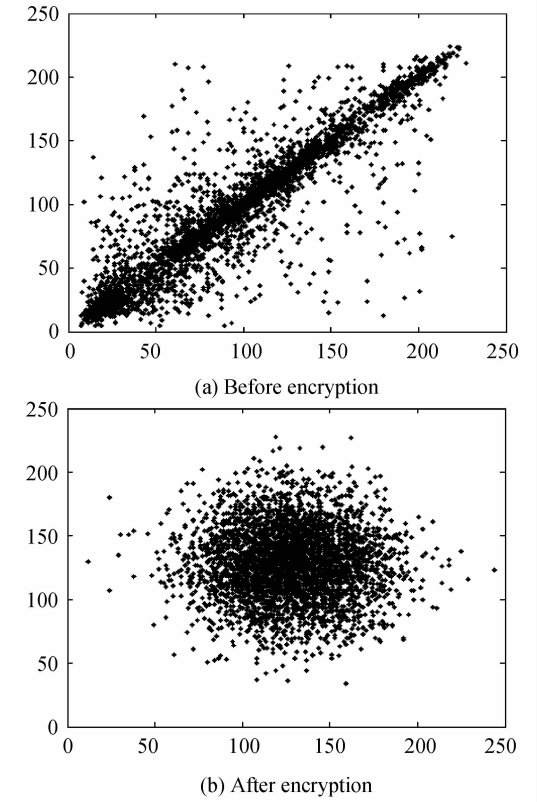


图 7　图像垂直方向像素相关性

Fig. 7　The pixel correlation in vertical direction

它们解密后的图像分别如图 8(b)，(d)所示，解密的图像基本都能分辨出人的轮廓和相貌特征. 因此本文方法对高斯噪音及椒盐噪音干扰具有一定的抵抗能力.

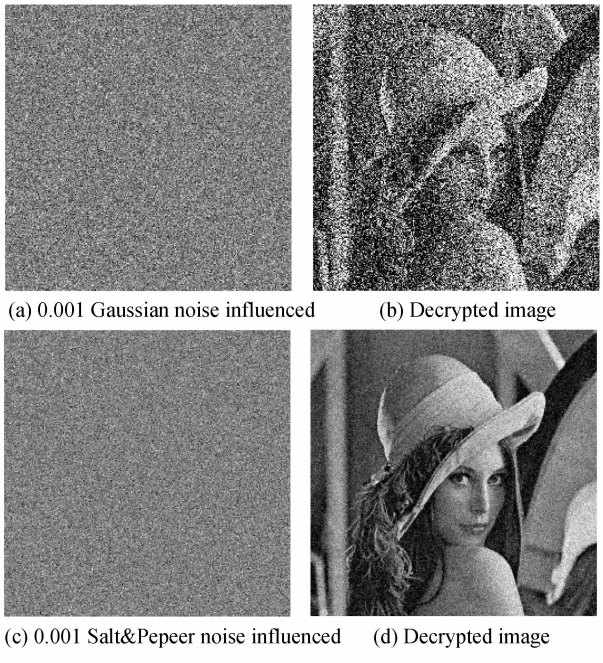


图 8　加性噪音干扰后的密文图像及解密图像

Fig. 8　The additive noise influenced image and the decrypted image

4 结论

针对光学中双随机相位图像加密方法的加密结果是复数而难以在数字图像加密中应用的问题，本文提出了一种叫做图像重构变换的方法来实现数字图像的双随机相位加密，并证明了这种算法的复杂度较低.实验结果表明该方案的加密图像具有较小的信息熵，安全性较强，并具有一定的抗加性噪音干扰的能力.

参考文献

[1] SYED F. Children of DES: a look at the advanced encryption standard[J]. *Network Security*, 2000, **2000**(9): 11-12.

[2] PHAN R C W. Reducing the exhaustive key search of the data encryption standard (DES)[J]. *Computer Standards & Interfaces*, 2007, **29**(5): 528-530.

[3] GONG Jin, LIU Wen-yi, ZHANG Hui-xin. Multiple lookup table-based AES encryption algorithm implementation [J]. *Physics Procedia*, 2012, **25**(0): 842-847.

[4] WANG Yuan-mei, LI Tao. Study on image encryption algorithm based on arnold transformation and chaotic system [C]. Proceedings of the 2010 International Conference on Intelligent System Design and Engineering Application. Orlando, Florida, USA: IEEE, 2010: 499-451.

[5] KUMAR G M B S S, CHANDRASEKARAN V. A novel image encryption scheme using Lorenz attractor [C]. Proceedings of the 4th IEEE Conference on Industrial Electronics and Applications. Orlando, Florida, USA: IEEE, 2009: 3662-3666.

[6] ZHU Ai-hong, LI Lian. Improving for chaotic image encryption algorithm based on logistic map[C]. Proceedings of the 2nd International Conference on Environmental Science and Information Application Technology. Orlando, Florida, USA: IEEE, 2010: 211-214.

[7] XIAO Yu, ZHANG Hai-ying , RAN Qi-wen, *et al*. Image encryption and two dimensional discrete M-parameter Fractional Fourier transform [C]. Proceedings of the 2nd International Congress on Image and Signal Processing. Orlando, Florida, USA: IEEE, 2009: 1-4.

[8] YOSHIMURA H, IWAI R. New encryption method of 2D image by use of the fractional Fourier transform [C]. Proceedings of the 9th International Conference on Signal Processing. Orlando, Florida, USA: IEEE, 2008: 2182-2184.

[9] WANG Ya-qing, ZHOU Shang-bo. A novel image encryption algorithm based on fractional Fourier transform [C]. Proceedings of the 2011 International Conference on Computer Science and Service System. Orlando, Florida, USA: IEEE, 2011: 72-75.

[10] SITU G, ZHANG Jing-juan. Double random-phase encoding in the Fresnel domain[J]. *Optics Letters*, 2004, **29**(14): 1584-1586.

[11] REFREGIER P, JAVIDI B. Optical image encryption based on input plane and Fourier plane random encoding[J]. *Optics Letters*, 1995, **20**(7): 767-769.

[12] JAVIDI B, AHOUZI E. Optical security system with Fourier plane encoding[J]. *Applied Optics*, 1998, **37**(26): 6247-6255.

[13] YU Li, ZHU Bang-he, LIU Shu-tian. Optical image encryption based on double phase encoding with Fractional Fourier transform[J]. *Acta Photonica Sinica*, 2001, **30**(7): 904-907.
于力，朱邦和，刘树田. 用于光学图象加密的分数傅里叶变换双相位编码[J]. 光子学报，2001，**30**(7)：904-907.

[14] LU Hong-qiang, ZHAO Jian-lin, FAN Qi, *et al*. Iterative double random phase encryption based on pixel scrambling technology[J]. *Acta Photonica Sinica*, 2005, **34**(7): 1069-1073.
陆红强，赵建林，范琦，等. 基于像素置乱技术的多重双随机相位加密法[J]. 光子学报，2005，**34**(7)：1069-1073.

[15] LI Rong, LI Ping. Research on the image security in double random phase real-value encryption [J]. *Acta Photonica Sinica*, 2005, **34**(6): 952-955.
李榕，李萍. 双随机相位图像加密的实值编码研究[J]. 光子学报，2005，**34**(6)：952-955.

[16] LI Ping, LI Rong. Real-value encryption for optical security system based on holography [J]. *Acta Photonica Sinica*, 2008, **37**(5): 957-959.
李萍，李榕. 基于全息技术的光学加密系统实值编码[J]. 光子学报，2008，**37**(5)：957-959.

[17] LI Xue-mei, RAN Tao, DAI Liu-ling, *et al*. Reality-preserving image encryption associated with the generalized Hilbert transform [C]. Proceedings of the 2009 IEEE International Symposium on Industrial Electronics. Orlando, Florida, USA: IEEE, 2009: 1909-1913.

[18] VENTURINI I, DUHAMEL P. Reality preserving fractional transforms[C]. Proceedings of the 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing. Orlando, Florida, USA: IEEE, 2004: 205-208.

[19] ZHU Zhi-liang, ZHANG Wei, WONG K W, *et al*. A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. *Information Sciences*, 2011, **181**(6): 1171-1186.

[20] WANG Yong, WONG K W, LIAO Xiao-feng, *et al*. A new chaos-based fast image encryption algorithm [J]. *Applied Soft Computing*, 2011, **11**(1): 514-522.

An Algorithm of Keeping Non-negative Integer Value in Image Encryption

LÜ Shan-xiang[1], WANG Zhao-shan[1], SHENG Yan[2], FENG Jiu-chao[1]
(1 *School of Electronic and Information Engineering, South China University of Technology, Guangzhou* 510641, *China*)
(2 *Guangzhou Marine Geological Survey bureau, Guangzhou* 510760, *China*)

Abstract: A novel image transforming method called Reconstruction Transform is proposed, which can make the double random phase encryption image become non-negative integer value. Reconstruction transform includes two stages, pre-processing and spectral shifting. It′s major characteristic is that, compress the interger image to become complex image of half-sized before applying spectral transform to the original image, thus reducing the calculation space in the following steps. The proposed method has the advantage of joint image compression and encryption. Compared with the chaotic image encryption scheme, the cipher-text image of the proposed scheme has lower information entropy. Experimental results show that this method has high security, the decrypted image of this method has little distortion and the cipher-text image has a certain degree of robustness to additive noise attack.

Key words: Optical image; Digital image; Complex value; Non-negative integer